NCIX
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Intelligence Community
Centers of Academic Excellence
Summer Seminar

24 July 2007

Remarks by

JOEL F. BRENNER

NATIONAL COUNTERINTELLIGENCE EXECUTIVE

"Intelligence, Thinking, and Academia"

Good afternoon, ladies and gentlemen. I am Joel Brenner, the National Counterintelligence Executive, in the Office of the Director of National Intelligence. I'm going to start by telling you what counterintelligence is and what I do, and then I'll explain why I asked for some of your time today.

Counterintelligence

Counterintelligence is the business of identifying and dealing with threats to the United States from the foreign intelligence services of foreign states and similar organiza-

tions of non-state actors –transnational terrorist groups such as al Qa'ida and Lebanese Hizbollah, for instance. We have both a defensive mission — protecting the nation's secrets and assets against foreign intelligence penetration — and an offensive mission — finding out what foreign intelligence organizations are up to in order to better defeat their aims.

By statute, Congress has charged me with promulgating a strategy for all U.S. counterintelligence elements. My office must (1) integrate activities of all our counterintelligence programs to make them coherent and efficient, (2) coordinate counterintelligence policy and budgets to same end, and (3) evaluate performance of counterintelligence community against the strategy. The key noun here is "strategy." The key verbs are "integrate", "coordinate", "evaluate." My office doesn't do operations.

Espionage

In my line of work, the standing joke is, if you're catching spies, you messed up, you failed. And if you're not catching spies, you're messing up, you're failing. Espionage is a persistent problem, and it wasn't an invention of the Cold War. It's older than Joshua's reconnoitering of the Promised

Land, and it will be with us forever. In case your memory requires refreshing, the United States has suffered our share of hostile penetrations in the last couple of decades:

- FBI agent Robert Hanssen spied for Soviets/Russians for two decades and gave them continuity of government information they could have used to defeat us decisively if war had broken out.

- Walker spy ring provided Soviets with cryptologic material that let them read more than a million messages to our ships and submarines at sea.

- Conrad spy ring compromised to Soviets war planning for defense of Europe. The judge at Conrad's trial wrote: "If war had broken out between NATO and the Warsaw Pact, the West would have faced certain defeat."

- CIA case officer Aldrich Ames compromised hundreds of CIA, DoD, and FBI human agent operations. Virtually our entire network against Soviets was *wiped out* — imprisoned or killed.

- DIA analyst Ana Montes caught after 15 years' spying against us for Cubans; compromised our entire program against Cuba — electronic as well as human.

These are cases of treason, and they still go on. Within the past few months a federal court in California found *Chi Mak* – a US citizen of Chinese origin – guilty in a case with profound implications for our military. For starters, he compromised the radar on the Navy's next generation (DDX) warship. Chi Mak wasn't a government employee; he was a contractor's employee, and he also worked on the Navy's quiet electric drive, designed to suppress signatures emitted by our submarines and surface warships. We lost this technology too. The technologies he compromised cost U.S. taxpayers billions to develop, and the Chinese got it free. What he did shortened by years the U.S. Navy's technological advantage. It degraded deterrent capability in Taiwan Strait. And it put the lives of our sons, daughters, and fellow citizens in the Navy at risk.

Preventing penetrations like these, and ferreting them out early when we can't prevent them, is a big part of coun-

terintelligence. The job isn't getting easier, I'm afraid. There are about 140 foreign intelligence services whose primary target is the United States and U.S. companies.

It's not getting easier to another reason, too. Nowadays, information is electrons, electrons travel on cyber network, and those networks are vulnerable. Our nation's electronic networks – and here I emphatically include those at every university represented in this room – are too easy to hack, while the number of world-class hackers is multiplying at bewildering speed. If you can exfiltrate massive amounts of information electronically from any place on earth, why incur the expense and risk of running a spy? If you can disrupt critical infrastructure electronically from the other side of the world, who needs a local saboteur? Our water and sewer systems, electricity grids, financial markets, payroll systems, air- and ground-traffic control systems – they're all electronically controlled, and they are subject to sophisticated attack by state-sponsored as well as free-lance hackers. This is not science fiction. If you want a preview of this sort of attack, just take note of the massive and effective attacks on Estonia emanating from Russia this spring. It was the first coordinated, denial-of-service attack directed at

the infrastructure of a nation-state, but it won't be the last. To my way of thinking, cyber network vulnerability is a new frontier for counterintelligence.

Counterintelligence, by the way, is not security. Let me put it this way. If there's a hole in your fence, security's job is to fix it. Our job (in part) is to figure out how it got there, who's been coming through it, and what they took when they left. We collaborate closely with security, but we're in a different line of work.

Common Agenda

What brings me here today, however, isn't fences. It's the strategic part of my work and our common agenda. The business of intelligence must be closely related with intelligence writ large, and that is why, strategically speaking, the relationship of the intelligence community with the academic community must remain vital. Our nation's well-being depends on it.

You also know from your own experience that, in all walks of life, urgent issues get immediate attention and that crises drive decision-making. But urgency and importance are not

the same thing, and there is a constant struggle in the world of policy-makers, and in the intelligence community that serves them, to pay attention to what's important even when it's not urgent. The more strategic the intellectual questions, the more intelligence analysts look like academics; and the more strategic the personnel questions, the more our interests converge. We both ask:

- How will the world look in five or ten or 20 years?

- What are the cultures, histories, politics, and languages that we in the intelligence community will wish we had begun studying now, in 2007 – *and that you in the universities will wish you had begun teaching now, in 2007* – rather than in 2015?

- What are the skill sets our engineers and computer scientists, our lawyers and psychologists will need in 2015?

Last week I had the pleasure of moderating a panel of distinguished professionals on the question of open-source information. The intelligence community, as you may know,

is sometimes accused of having an unwarranted bias in favor of the secret over the open, and this panel was part of a conference designed to address that issue. It included a lawyer, an executive of a polling organization, a journalist now in the consulting business, and an experienced policy advisor now in academia. When all of them had finished speaking, I realized (and noted) that each of them had spoken only about what we need to know about the present or future, and that none of them had mentioned history as being open-source information worth having. Those of us in the business of strategic intelligence, however, must know – and here I am quoting the late, brilliant Adda Bozeman of Sarah Lawrence College – that "all human contests are in the final analysis mental and psychological, and … can be won or managed only by those who understand the mind-set of the counterplayer while being resolutely certain of just who they are themselves and what it is they stand for." The other occupants of this planet are not all Americans under the skin. They behave differently than we do, and they think differently than we do. And their mind-sets are historically conditioned. To that end, Bozeman was right to insist that "history must be accepted as the primary and indispensable tool of political analysis …." Your graduates who are well

trained in history, politics, and languages are going to find work in our agencies.

At the same time, the intelligence community's appetite for engineers, computer scientists, and other technical specialists will continue to be insatiable. (By the way, I hope you won't regard the realm of the humanities and the realm of the physical sciences as mutually exclusive. It may be too much to *demand* graduates steeped in both, but we do get some. They are treasures, and they write their own tickets.)

Lately I've been asked about programs in national security, or homeland security, and how they should be set up. Let me say, first, that it's immensely gratifying to those of us in the intelligence community to see the flowering of interest in strategic and security studies; and, second, that there's no one right way to set up these programs. So I'll make just one suggestion. If your institution is thinking along these lines, either to start a new program or expand an existing one, then build on what you already have. An institution with a strong program in nursing or public health, for example, is likely to pursue an angle that may be quite different from another school with strong area studies in,

say, Africa or Latin America. Relevance is what you make of it. A school with a solid program in electrical engineering, but weak in area studies or political theory, has possibilities to develop a program in cyber network security that the other won't have. Figure out your strong suit, and play to it.

Now, as to counterintelligence in particular, I can't resist pointing out that no national security program that I know of is built around this topic, and very few pay any attention to it at all. To help remedy that, my Office is supporting an effort at the National Defense University to create and, so to speak, test drive a counterintelligence course. I'm hoping that we may have it ready to go in about three semesters – after which we will make the syllabus, outline, and reading list available to any program that wants it. So stay tuned.

In closing, let me thank you for your interest in this seminar. Our nation is engaged in what promises to be a long struggle against a foe that relentlessly de-humanizes it enemies. This struggle will require our imagination, our will power, and our intelligence. Our task as citizens is to align our institutions to support American vitality, safety, and security, and to do it in a way that is methodical but not

hysterical, bold but not imprudent, forceful but not intolerant. We need each other. Thank you.

###